

Response to First Office Action  
Docket No. 002.0132.US.UTL

Amendments to the Claims

This listing of claims will ~~replace~~ all prior versions, and listings, of claims in the application:

Listing of Claims:

- 1 1. (currently amended): A system for dynamically detecting computer  
2 viruses through associative behavioral analysis of runtime state, comprising:  
3 a parameter set stored on a client system defining a group of monitored  
4 ~~events which each comprise, each monitored event comprising~~ a set of one or  
5 more actions defined within an object, each action being performed by one or  
6 more applications executing within a defined computing environment;  
7 a monitor executing on the client system, comprising:  
8 a collector continuously monitoring ~~[[the]]~~ runtime state within the  
9 defined computing environment for an occurrence of any one of the monitored  
10 events in the group and tracking ~~[[the]]~~ a sequence of ~~[[the]]~~ execution of the  
11 monitored events for each of the applications; and  
12 an analyzer identifying each occurrence of a specific event  
13 sequence characteristic of ~~computer virus behavior~~ of a computer virus and the  
14 application which performed the specific event sequence, creating a histogram  
15 describing the specific event sequence occurrence for each of the applications,  
16 and identifying repetitions of the histogram associated with at least one object.
- 1 2. (original): A system according to Claim 1, further comprising:  
2 a storage manager organizing the histograms into plurality of records  
3 ordered by object, application, and monitored event.
- 1 3. (original): A system according to Claim 2, further comprising:  
2 a structured database in which the plurality of records is stored; and  
3 the storage manager storing each histogram for each such specific event  
4 sequence occurrence in one such database record identified by the application by  
5 which the specific event sequence was performed.

Response to First Office Action  
Docket No. 002.0132.US.UTL

- Q2
- 1 4. (original): A system according to Claim 3, further comprising:  
2 the storage manager configuring the structured database as an event log  
3 organized by each event in the group of monitored events and updating the  
4 database record storing each specific event sequence occurrence with a revised  
5 histogram as each such occurrence is identified.
- 1 5. (original): A system according to Claim 1, further comprising:  
2 the analyzer detecting suspect activities within each histogram, each  
3 suspect activity comprising a set of known actions comprising a computer virus  
4 signature.
- 1 6. (currently amended): A system according to Claim ~~[[6]]~~5, wherein  
2 each such suspect activity is selected from ~~[[the]]~~a class of actions comprising file  
3 accesses, program executions, message transmissions, configuration area  
4 accesses, security setting accesses, and impersonations.
- 1 7. (currently amended): A system according to Claim 6, wherein each  
2 such suspect activity is selected from ~~[[the]]~~a group comprising files accesses,  
3 program executions, direct disk accesses, media formatting operations, sending of  
4 electronic mail, system configuration area accesses, changes to security settings,  
5 impersonations, and system calls having the ability to monitor system  
6 input/output activities.
- 1 8. (currently amended): A system according to Claim 1, wherein the  
2 computer virus comprises at least one form of unauthorized content selected from  
3 ~~[[the]]~~a group comprising a computer virus application, a Trojan horse  
4 application, and a hoax application.
- 1 9. (currently amended): A method for dynamically detecting  
2 computer viruses through associative behavioral analysis of runtime state,  
3 comprising:

Response to First Office Action  
Docket No. 002.0132.US.UTL

4 defining a group of monitored events ~~which each comprise, each~~  
5 monitored event comprising a set of one or more actions defined within an object,  
6 each action being performed by one or more applications executing within a  
7 defined computing environment;  
8 continuously monitoring ~~[[the]]~~ runtime state within the defined  
9 computing environment for an occurrence of any one of the monitored events in  
10 the group;  
11 tracking ~~[[the]]~~ a sequence of ~~[[the]]~~ execution of the monitored events for  
12 each of the applications;  
13 identifying each occurrence of a specific event sequence characteristic of  
14 ~~computer virus~~ behavior of a computer virus and the application which performed  
15 the specific event sequence;  
16 creating a histogram describing the specific event sequence occurrence for  
17 each of the applications; and  
18 identifying repetitions of the histogram associated with at least one object.

1 10. (original): A method according to Claim 9, further comprising:  
2 organizing the histograms into plurality of records ordered by object,  
3 application, and monitored event.

1 11. (original): A method according to Claim 10, further comprising:  
2 maintaining a structured database in which the plurality of records is  
3 stored; and  
4 storing each histogram for each such specific event sequence occurrence  
5 in one such database record identified by the application by which the specific  
6 event sequence was performed.

1 12. (original): A method according to Claim 11, further comprising:  
2 configuring the structured database as an event log organized by each  
3 event in the group of monitored events; and

Response to First Office Action  
Docket No. 002.0132.US.UTL

4 updating the database record storing each specific event sequence  
5 occurrence with a revised histogram as each such occurrence is identified.

1 13. (original): A method according to Claim 9, further comprising:  
2 detecting suspect activities within each histogram, each suspect activity  
3 comprising a set of known actions comprising a computer virus signature.

1 14. (currently amended): A method according to Claim 13, wherein  
2 each such suspect activity is selected from ~~[[the]]~~ a class of actions comprising file  
3 accesses, program executions, message transmissions, configuration area  
4 accesses, security setting accesses, and impersonations.

1 15. (currently amended): A method according to Claim 13, wherein  
2 each such suspect activity is selected from ~~[[the]]~~ a group comprising files  
3 accesses, program executions, direct disk accesses, media formatting operations,  
4 sending of electronic mail, system configuration area accesses, changes to  
5 security settings, impersonations, and system calls having the ability to monitor  
6 system input/output activities.

1 16. (currently amended): A method according to Claim 9, wherein the  
2 computer virus comprises at least one form of unauthorized content selected from  
3 ~~[[the]]~~ a group comprising a computer virus application, a Trojan horse  
4 application, and a hoax application.

1 17. (currently amended): A computer-readable storage medium  
2 holding code for dynamically detecting computer viruses through associative  
3 behavioral analysis of runtime state, comprising:  
4 defining a group of monitored events ~~which each comprise~~ each  
5 monitored event comprising a set of one or more actions defined within an object,  
6 each action being performed by one or more applications executing within a  
7 defined computing environment;

Response to First Office Action  
Docket No. 002.0132.US.UTL

Q2


8 continuously monitoring ~~[[the]]~~ runtime state within the defined  
9 computing environment for an occurrence of any one of the monitored events in  
10 the group;  
11 tracking ~~[[the]]~~ a sequence of ~~[[the]]~~ execution of the monitored events for  
12 each of the applications;  
13 identifying each occurrence of a specific event sequence characteristic of  
14 ~~computer virus~~ behavior of a computer virus and the application which performed  
15 the specific event sequence;  
16 creating a histogram describing the specific event sequence occurrence for  
17 each of the applications; and  
18 identifying repetitions of the histogram associated with at least one object.

1 18. (original): A storage medium according to Claim 17, further  
2 comprising:  
3 organizing the histograms into plurality of records ordered by object,  
4 application, and monitored event.

1 19. (original): A storage medium according to Claim 18, further  
2 comprising:  
3 maintaining a structured database in which the plurality of records is  
4 stored; and  
5 storing each histogram for each such specific event sequence occurrence  
6 in one such database record identified by the application by which the specific  
7 event sequence was performed.

1 20. (original): A storage medium according to Claim 19, further  
2 comprising:  
3 configuring the structured database as an event log organized by each  
4 event in the group of monitored events; and  
5 updating the database record storing each specific event sequence  
6 occurrence with a revised histogram as each such occurrence is identified.

Response to First Office Action  
Docket No. 002.0132.US.UTL

- 
- 1            21.    (original): A storage medium according to Claim 17, further  
2    comprising:  
3            detecting suspect activities within each histogram, each suspect activity  
4    comprising a set of known actions comprising a computer virus signature.
-